REMARKS

This Response is submitted in response to the Office Action dated June 21, 2007. The original unamended claimset consisting of claims 1-24 remains pending.

CLAIM REJECTIONS UNDER 35 U.S.C. §§ 102 AND 103:

Claims 1-4, 9-12, and 17-20 have been rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Pat. App. No. 2002/0099837, filed by Oe et al. (hereinafter *Oe*). Claims 5-8, 13-16, and 21-24 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over *Oe* as applied to claims 1, 9, and 17, and in further view of U.S. Pat. App. No. 2004/0064572, filed by Yamaguchi et al. (hereinafter *Yamaguchi*). Applicants respectfully traverse the foregoing rejections of claims 1-4, 9-12, and 17-20 under 35 U.S.C. § 102(b) for the following reasons.

Applicants' proposed invention addresses security issues relating to transferring data from a data processing system onto a network. As explained in Applicants' Background, security issues with such transfers are generally addressed by user authorization methods and/or by using access control list (ACL) enforcement in which an ACL is maintained for each "resource" (e.g. file or data object), with the ACL recording authorized actions and/or users. However, as noted in Applicants' Background, such resource-associated ACL techniques may not prevent illegitimate data transfers from a Trojan horse program that was able to conceal its identity when it entered the system.

As recited in independent claims 1, 9, and 17 Applicants' proposed invention substantially modifies the conventional ACL approach which focuses on maintaining a list of authorized actions/users for particular files. Namely, Applicants' invention first implements a data file and process tracking mechanism fundamentally comprising: (1) identifying a list of data files to be protected ("creating a file list of one or more data files to be controlled"); and (2) generating a process list associated with each of the identified data files ("creating a process list for each data file in the file list"), wherein the process list lists each process that has accessed the data file in question ("wherein each process list identifies one or more processes executing in the data processing system that has accessed the data file associated with the created process list"). Having established this tracking mechanism that tracks access of sensitive data files by particular processes, the invention then applies a security procedure for each attempted data transfer from the data processing system in which responsive to a request to transfer data to a network, the requesting process is matched against the process lists for the tracked data files ("determining if the requesting process is identified in one or more created process lists"). If the requesting process is identified as being included in one of the process lists, the request is initially prohibited ("if the requesting process is identified in a created process list, prohibiting the requested transfer of data from the data processing system to the network").

As further recited in dependent claims 5-7, 13-15, and 21-23, prohibiting the network data transfer request in accordance with this mechanism enables a user or other subsequent authorization sequence to ensure the security of the transfer.

Oe's disclosure relates generally to a computer resource access control technique having a "trap" feature in which a resource request is trapped pending the outcome of an access determination (see Abstract, page 1, paragraphs [0010]-[0013]). As asserted on page 2 of the Office Action, *Oe* discloses a method for controlling data transfer including a step of creating a file list of one or more data files to be controlled. Namely, page 1, para. [0015] describes the file list as an "access right management table" containing resource designation information that designates a specific computer resource, condition information under which the access right is validated, and access right information that designates an access right.

Next, the Office Action asserts that *Oe* discloses "creating a process list for each data file in the file list, wherein each process list identifies one or more processes executing in the data processing system that has accessed the data file associated with the created process list" (**FIG. 8** and page 15, paragraph [0348]). Applicants respectfully disagree. The access monitoring log depicted and described in **FIG. 8** and paragraph [0348] includes row-wise entries specifying for a given file, a user and an operation (e.g. file move), but nowhere does *Oe* specify that the process "list" (i.e., the "operation" entry for each respective listed file in the access monitor log) is a process list for each data file in the "file list." Consistent with the Office Action's identification of the subject matter on page 1, paragraph [0015] as disclosing "the file list", each "operation" entry in the log depicted in **FIG. 8** would have to be a process "list" for each data file in the "access right management table." Such correlation between the "file list" and "process list" is required by Applicants' express claim language and is an important feature in achieving the necessary surveillance over the files specified in the "file list." No such correlation is made by *Oe* since *Oe's* procedure is substantially different than Applicants'.

Applicants further disagree that *Oe* discloses a step of determining if the requesting process (i.e. a process requesting a network data transfer) is identified in one or more created process lists. Page 1, paragraph [0011] generally describes a determination of "whether an access right for the computer resource designated by the operation request trapped in the trap step is present" with no mention or suggestion of determining whether a requesting processing is contained in a "process list" defined in accordance with the above-mentioned claim elements. Consistent with the Office Action's cite to the aforementioned "access monitor log" depicted in **FIG. 8** as disclosing the "process lists," any determination by *Oe* of whether a requesting process is included in a process list should have some relation to the "operations" column of the access monitor log in **FIG. 8**.

Applicants have diligently explained in detail why the present claims are distinct over the prior art and particularly why the present grounds for rejecting independent claims 1, 9, and 17 should be withdrawn. Applicants therefore believe that pending claims 1, 9, 17, and all claims depending therefrom are in condition for allowance and respectfully request a notice to that effect. Furthermore, Applicants invite the Examiner to contact the undersigned attorney of record at (512) 343-6116 if such would further or expedite the prosecution of the present Application.

Respectfully submitted,

Matthew W. Baca
Reg. No. 42,277
DILLON & YUDELL LLP
8911 North Capital of Texas Highway, Ste. 2110
Austin, Texas 78759
Telephone (512) 343-6116
Facsimile (512) 343-6446

ATTORNEY FOR APPLICANTS